REMARKS

The Office Action dated January 15, 2004 has been received and carefully considered. The above amendments and the following remarks are being submitted as a full and complete response to the Office Action.

Claim 14 has been cancelled and the full features thereof incorporated into independent claim 1. Claims 15, 16, 19, 22, and 25 to 27 have been canceled, and the features thereof incorporated into claims 6 through 12, each of which depends from amended claim 1. According to the above amendments, independent claim 1 has been amended to emphasize the following important features of the present invention.

1. The attack detecting means is disposed at a gateway of the network, for successively acquiring IP packets passing through the gateway, storing the acquired IP packets accumulatively, and monitoring the stored IP packets while the gateway remains open to detect a cracker attack against the network.

2. The processing means of the present invention comprises means for preventing an IP packet having a source IP address and/or a destination IP address associated with the attack detected by the attack detecting means, from entering the network in the predetermined process, for a predetermined time after the attack detecting means detects the attack.

More specifically, in accordance with the present invention, the IP packets continue to pass through a gateway, while the IP packets are acquired and stored at a location remote from the gateway per se. When searching the IP packets for potential attacks, rather than monitoring the IP packets at the gateway access point, the stored IP packets are monitored at the remote location, while the gateway remains open to IP traffic.

Then, only after a certain threshold number of stored IP packets, which have already passed the gateway and have been stored, are determined to represent malicious attacking behavior, then the gateway is closed to such IP packets. According to this feature of the invention, i.e., by maintaining an open gateway and monitoring stored IP packets at a location remote from the gateway, the gateway can remain open as long as possible to non-offending IP traffic. In other words, the gateway is not shut off to malicious IP traffic immediately and in all instances to prevent passage of such IP packets through the gateway. Rather, IP packets are allowed to pass through the gateway, while the packets are monitored and examined for cracker attacks at a stored location. Thus, essentially all traffic is allowed to pass and continue through the gateway, for as long a time as possible, until a malicious attack is discovered from among the stored IP packets.

Secondly, once an attack is detected from among the stored IP packets, only then the IP packets associated with the attack are prevented from entering the gateway, and only then for a predetermined period of time. Moreover, as set forth in the dependent claims, the predetermined time period may depend, in a flexible manner, on the type of attack. Thus, unlike traditional firewall protections, IP packets associated with the attack are not shut off completely, but rather, the ingress of the IP packets is prevented for a predetermined time period sufficient to stop the attack, and thereafter, the gateway is reopened.

More specifically, the present invention recognizes that IP packets having given destination/source addresses may be used *at times* for mounting malicious cracker attacks. However, at other times, well-intentioned users can use the same IP packets bearing the same source/destination addresses without malice. Thus, it would be overly restrictive to continuously prohibit access at the gateway to such IP packets. Rather, according to the claimed invention, such IP packets are prevented from passing the gateway only for a sufficient period of time to prevent success of the attack. Once the threat of attack is abated, then the gateway is reopened to such IP packets.

Therefore, contrary to traditional firewall prevention, which simply prevents ingress at all times of potentially malicious IP packets through a gateway, the present invention provides a flexible and adaptive technique, which monitors IP packets in a stored location while keeping the gateway open to traffic. When an attack is detected, the gateway is then shut down to prevent ingress of IP packets mounting the attack, but only for a predetermined period of time sufficient to prevent the attack, and thereafter, the gateway is reopened to such IP packets. Thus, the goal of the invention is to enable the gateway to remain open to all traffic, to the greatest extent possible, while still preventing cracker attacks during times when the attacks are being mounted.

In addition to claim 1, independent claim 28 includes the same features discussed above. In particular, according to claim 28, acquired and stored IP packets are monitored while the

gateway remains open, to detect cracker attacks from the acquired and stored IP packets based on an algorithm, and IP packets are prevented from entering the network according to a predetermined process, for a time which is predetermined corresponding to the detected type of attack, after the attack detecting means detects one of the attacks. Again, once the threat of attack is abated, the gateway is reopened to such IP packets. Accordingly, claim 28 is allowable over the cited prior art, essentially for the same reasons as claim 1.

It is respectfully submitted that the cited prior art provides no suggestion for the features of the claimed invention, and does not enable the advantages highlighted above, as shall now be discussed below.

Claims 1-4 and 13 were rejected under 35 U.S.C. § 102(b) as being anticipated by Escamillia.

Since claim 14 (the features of which are now presented in claim 1) and claim 28 were not included in the above rejection, it is submitted that the rejection is moot with respect to the amended claims. However, Escamillia does not suggest the feature of monitoring stored IP packets, at a location remote from the gateway, while the gateway remains open to IP traffic, as discussed above.

With respect to acquiring/storing IP packets, in the Office Action the Examiner references Escamillia, page 147 and the paragraph entitled "Data Source."

Actually, there is no explicit mention in the indicated paragraph of storing IP packets having passed through a gateway.

This section of the reference generally refers to the need to monitor the log files that are automatically generated in a server (e.g., Unix) environment. There is no discussion whatsoever of storing IP packets that have passed through a gateway, monitoring the IP packets at the stored location remote from the gateway while the gateway remains open, and then preventing an IP packet from entering the network only for a predetermined of time, after which the gateway is reopened. The relationship of the gateway to the monitoring method is not addressed at all in Escamillia.

Claims 5, 6-12 and 14-29 were rejected under 35 U.S.C. 103(a) as being unpatentable over Escamillia in view of Cheswick.

Cheswick generally address various firewall features, which involve monitoring and classifying IP packets according to various techniques.

However, again, the cited reference does not appreciate the relationship between the openness of the gateway (i.e., keeping the gateway open to all IP traffic as much as possible) and the monitoring method being conducted at a stored location remote from the gateway. Cheswick also does not suggest the feature of closing the gateway to malicious IP packets only for a predetermined period of time.

Summarizing, the references discuss certain criteria upon the contents of data (IP) packets including source and destination addresses. However, the references do not disclose a system in which even malicious data packets, having unallowable addresses, can pass through the gateway to the network. By

contrast, according to the present invention, a cracker attack is detected by acquiring successively IP packets passing through a gateway of a network, storing the acquired IP packets accumulatively, and monitoring the stored IP packets at the stored location remote from the gateway. Even malicious IP packets related to a cracker attack are allowed to pass through the network until the malicious IP packets included in the stored IP packets reaches a predetermined threshold. Thus, the network is maintained accessible as much as possible for good IP packets having no relationship with the cracker attack.

Further, in the present invention, even when a cracker attack is detected, the gateway is closed to unallowable IP addresses, and such IP addresses cannot pass to the network only for a predetermined period of time. According to the present invention, if a cracker attack is detected, then a predetermined process is performed for a time which is predetermined depending on the type of the detected attack. In other words, the claimed invention acts as a flexible antibody for destroying each of several types of antigens (attacks) in the most suitable way, in the shortest amount of time possible, without routinely and continuously shutting down a gateway simply to designated IP packets.

Accordingly, the applicant respectfully submits that the claimed invention is both novel and non-obvious over the cited prior art. Withdrawal of the rejections is requested.

A petition to extend the respond period for replying to the Office Action for three months, until August 15, 2004,

accompanies this response. Otherwise, fees are not due. Notwithstanding, should it be deemed that other fees, or deficiencies in fees, are required in connection with this or any accompanying communication, such amounts may be charged to the Attorney's Deposit Account No. 07-2519.

Respectfully submitted,

Paul A. Guss
Reg. No. 33,099
Attorney for Applicants

CS-02-000131

775 S. 23rd St. #2
Arlington, VA 22202
Tel. 703-486-2710